M. Anderson Berry (SBN 262879)
Leslie Guillon (SBN 222400)
CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 777-7777
Facsimile: (916) 924-1829
ABerry@Justice4You.com
LGuillon@Justice4You.com

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

WILLIAM RIGGS, an individual and Florida resident, on behalf of himself and all others similarly situated, Plaintiff, vs. KROTO, INC., D/B/A ICANVAS, Defendant.	Case No.: _____ **CLASS ACTION COMPLAINT** DEMAND FOR JURY TRIAL

Plaintiff, William Riggs ("Plaintiff") brings this Class Action Complaint against Defendant Kroto, Inc. d/b/a iCanvas ("iCanvas") as an individual and on behalf of all others similarly situated, and alleges, upon personal knowledge as to his own actions and his counsels' investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. iCanvas specializes in selling canvas image and art prints through its website, www.icanvas.com. The company claims "Everyone can find something they will love, from graffiti street art to fine art." On information and belief, iCanvas uses an in-house ecommerce platform to take customers' personal and payment information.

2. On or about June 24, 2020, iCanvas began notifying customers and state Attorneys

General about a data breach that occurred from May 10 to 28, 2020 (the "Data Breach"). Hackers not only "scraped" many of iCanvas' customers' names from Defendant's website by infecting the ecommerce platform with malware, hackers also stole customers' payment card numbers, CVV security codes, credit card expiration dates, addresses, telephone numbers and email addresses ("PII"). The criminals obtained everything they needed to illegally use iCanvas' customers' payment cards to make fraudulent purchases, and to steal the customers' identities.

3. Not only did hackers skim iCanvas' customers' PII, on information and belief the stolen names and payment card information are now for sale on the dark web. That means the Data Breach worked. Hackers accessed and then offered for sale the unencrypted, unredacted stolen PII to criminals. Because of Defendant's Data Breach, customers' PII is still available on the dark web for criminals to access and abuse. iCanvas' customers face a lifetime risk of identity theft.

4. This PII was compromised due to iCanvas' negligent and/or careless acts and omissions and the failure to protect customers' data.

5. The stolen PII has great value to hackers: It is likely that hundreds of thousands of art lovers—residents of most states—were affected by the Data Breach. For example, so far iCanvas has filed data breach notices in California, Indiana, Massachusetts and Montana, among others.[1]

6. Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to: (i) adequately protect its users' PII; (ii) warn users of its inadequate information security practices; and (iii) effectively monitor iCanvas' websites and ecommerce platforms for security vulnerabilities and incidents. Defendant's conduct amounts to negligence and violates several states' statutes.

7. Plaintiff and similarly situated iCanvas customers ("Class Members") have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery

[1] *See, e.g.,* Exhibit 1, iCanvas' *Notice of Data Breach,* archived by the California Attorney General on June 24, 2020, *available at*: https://oag.ca.gov/system/files/Version%201%20-%20Notice%20of%20Data%20Breach.pdf (last accessed July 8, 2020).

from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, (iv) deprivation of rights they possess under Florida's Deceptive and Unfair Trade Practices Act (Florida Statute § 501.203, *et seq.*); and (v) the continued and certainly an increased risk to their PII, which: (a) remains available on the dark web for individuals to access and abuse; and (b) remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

II. PARTIES

8. Plaintiff William Riggs is a citizen of Florida residing in Polk County, Florida. Mr. Riggs purchased iCanvas products on May 27, 2020 using his Discover credit card. He received iCanvas' *Notice of Data Breach* or about June 26, 2020.

9. Defendant Kroto, Inc. is an Illinois corporation operating under the fictitious business name "iCanvas." Its principle place of business is located at 8280 Austin Ave., Morton Grove, Illinois. iCanvas advertises and sells goods to residents nationwide through its website and various retailers.

III. JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant. Plaintiff is a citizen of Florida and therefore diverse from iCanvas, which is headquartered in Illinois.

11. Defendant is subject to the personal jurisdiction of the Court because it does or transacts business in, has agents in, or is otherwise found in and has purposely availed itself of the privilege of doing business in California and in this District, and because the alleged misconduct was directed to California and this District, among others. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(1)-(3) because a substantial part of the events or omissions giving rise to

the claims occurred or were intentionally directed to residents and customers in this District.

IV. FACTUAL ALLEGATIONS

Background

12. iCanvas was founded in 2006 by its current CEO, Leon Oks. The canvas prints that iCanvas sells through its website and various retailers, including Home Depot, include modern photographs and classic works of art, including Van Gogh and Picasso. Customers will also find ready-to-hang canvases by such contemporary names as Banksy and finger-painter Iris Scott.

13. Customers purchasing online demand security to safeguard their PII. iCanvas touts the secure nature of its website in its Privacy Policy:

> **Our Commitment To You**
>
> At iCanvas, we value and respect your privacy. Privacy considerations are at the core of the way we design and build services for you so that you can fully trust iCanvas and take advantage of everything the Service offers. We do not compromise when it comes to your privacy, we seek to be transparent with you in the way we process and manage your personal information, and we work hard to protect your information and keep it secure[.][2]
>
> …
>
> **How We Protect Your Information**
>
> We strive to maintain internal controls and procedures to ensure that the information you share with us is handled in a safe, secure and responsible manner. We have implemented the appropriate technological and organizational measures necessary to help protect against the loss, unauthorized access and alteration of the information in our control.

14. iCanvas further reassures its customers in the FAQ section of its website[3]:

> **Security & Privacy**
>
> Is your website secure?
>
> Protecting your private data is our highest priority. We provide high-level protection through SSL, short for Secure Sockets Layer. This advanced cryptographic system is designed to encrypt private data so that it can be transmitted safely and securely over the Internet. SSL is the approved standard of the Internet Engineering Task Force (IETF). Our security system also meets the rigorous security requirements of the Payment Card Industry Data Security Standard (PCI DSS). As part of the order process, iCanvas will ask for your name, shipping/billing address, email, phone number, and your credit/debit (or another payment type)

[2] Exhibit 2, iCanvas' Privacy Policy.
[3] Exhibit 3, iCanvas' Security & Privacy statement (FAQ).

> information. This information will only be used for the purchase transaction and will never be given out to other businesses.

15. The PCI DSS (Payment Card Industry Data Security Standard) compliance is a requirement for businesses that store, process, or transmit payment card data. The PCI DSS defines measures for ensuring data protection and consistent security processes and procedures around online financial transactions.

16. As formulated by the PCI Security Standards Council, the mandates of PCI DSS compliance include, in part: Developing and maintaining a security policy that covers all aspects of the business, installing firewalls to protect data, and encrypting cardholder data that is transmitted over public networks using anti-virus software and updating it regularly.[4]

17. To purchase products on iCanvas' website, customers can create an account or check out as a guest. To complete a purchase, at a minimum, the customer must enter the following PII:

- Name;
- billing address;
- delivery address;
- email address;
- telephone number;
- name on the payment card;
- type of payment card;
- full payment card number;
- payment card expiration date; and
- security code, or CVV code (card verification number).

18. At no time during the final checkout process does iCanvas require customers to expressly agree to "Terms of Use," "Terms of Service" or "Terms & Conditions."

The Data Breach

19. Beginning on or about June 26, 2020, iCanvas sent customers a *Notice of Data Breach* signed by the founder and CEO, Leon Oks.[5] Oks informed the recipients of the notice that:

[4] PCI Security Standards Council, *available at*: https://www.pcisecuritystandards.org/ (last accessed July 8, 2020).
[5] Exhibit 1, p. 1.

> **WHAT HAPPENED?**
> On May 28, 2020, we discovered that unauthorized script was placed on the checkout page of the iCanvas Website. The unauthorized script potentially allowed the third party that placed the script to capture information submitted by customers on the checkout page of the iCanvas Website if the customer was paying using our credit card payment function and the "place your order" button was hit. Through our investigations, we discovered that the unauthorized script was likely placed on the iCanvas Website on or about May 10, 2020.
>
> **WHAT INFORMATION WAS INVOLVED?**
> The information potentially involved was limited to: First Name; Last Name; Street Address; City; State; Zip/Postal Code; Country; Phone Number; Email Address; Payment Card Number; Payment Card Security Code; and Payment Card Month/Year of Expiration, if the values for these items were entered while using the credit card payment function on the checkout page on the iCanvas Website and the "place your order" button was hit.

20. iCanvas' customers' information is likely for sale on the dark web and, on information and belief, is still for sale to criminals. This means that the Data Breach was successful; unauthorized individuals accessed iCanvas' customers' unencrypted, unredacted information, including "Name; Street Address; City; State; Zip/Postal Code; Country; Phone Number; Email Address; Payment Card Number; Payment Card Security Code; and Payment Card Month/Year of Expiration," and possibly more, without alerting Defendant, then offered the "scraped" information for sale online. There is no indication that Defendant's customers' PII was removed from the dark web where it likely remains.

21. Not long before iCanvas admits hackers were scraping its customers' PII, the FBI issued yet another warning to companies about this exact type of fraud. In the FBI's *Oregon FBI Tech Tuesday: Building a Digital Defense Against E-Skimming*, dated October 22, 2019, the agency stated:

> This warning is specifically targeted to . . . businesses . . . that take credit card payments online. E-skimming occurs when cyber criminals inject malicious code onto a website. The bad actor may have gained access via a phishing attack targeting your employees—or through a vulnerable third-party vendor attached to your company's server.

22. The FBI gave some stern advice to companies like iCanvas:

> Here's what businesses and agencies can do to protect themselves:
> - Update and patch all systems with the latest security software.
> - Anti-virus and anti-malware need to be up-to-date and firewalls strong.

- Change default login credentials on all systems.
- Educate employees about safe cyber practices. Most importantly, do not click on links or unexpected attachments in messages.
- Segregate and segment network systems to limit how easily cyber criminals can move from one to another.

23. But Defendant apparently did not take this advice: hackers scraped customers' PII off its website—and continued to do so until at least May 28, 2020.

24. Web scraping or skimming data breaches are commonly made possible through a vulnerability in a website or its backend content management system. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were collecting, causing customers' PII to be exposed and sold on the dark web.

Scraping and E-Skimming Breaches

25. *Magecart* is a loose affiliation of hacker groups responsible for skimming payment card attacks on various high-profile companies, including British Airways and Ticketmaster.[6] Typically, these hackers insert virtual credit card skimmers or scrapers (also known as *formjacking*) into a web application (usually the shopping cart), and proceed to scrape credit card information to sell on the dark web.[7]

26. The hackers target what they refer to as the *fullz*; a term used by criminals to refer to stealing the full primary account number, card holder contact information, credit card number, CVV security code and expiration date. The *fullz* is exactly what iCanvas admits the malware infecting its ecommerce platform scraped.

27. These cyber-attacks exploit weaknesses in the code of the ecommerce platform, without necessarily comprising the victim websites' networks or servers.[8] These attacks have targeted payment processors, but the attack on British Airways in 2018 was far more tailored to the company's particular infrastructure, as may be the case here.[9]

---

[6] *Magecart Hits 80 Major eCommerce Sites in Card-Skimming Bonanza*, Threatpost, Aug. 28, 2019, *available at*: https://threatpost.com/magecart-ecommerce-card-skimming-bonanza/147765/ (last accessed July 8, 2020).

[7] *Id.*

[8] *What is Magecart and was it behind the Ticketmaster and BA hacks?*, Computerworld, Sep. 18, 2018, *available at*: https://www.computerworld.com/article/3427858/what-is-magecart-and-was-it-behind-the-ticketmaster-and-ba-hacks-.html (last accessed July 8, 2020).

[9] *Id.*

28. Magecart and these scraping breaches are not new: RiskIQ's earliest Magecart observation occurred on August 8th, 2010.[10] Since it's been going on for almost a decade, and with the well-publicized and widespread attacks on British Airways and Ticketmaster, among many others in and since 2018, Defendant should have known the imminent danger facing its customers.

29. Unfortunately, despite all of the publicly available information of the continued compromises of PII in this manner, including the FBI's current warnings, Defendant's approach to maintaining the privacy and security of Plaintiff's and Class Members' PII was negligent, or at the very least, Defendant did not maintain reasonable security procedures and practices appropriate to the nature of the information to protect its customers' valuable PII.[11]

Value of Personally Identifiable Information

30. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[12] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web; the *fullz* sold for $30 in 2017.[13] Criminals

---

[10] *Magecart: New Research Shows the State of a Growing Threat*, RiskIQ, Oct. 4, 2019, *available at*: https://www.riskiq.com/blog/external-threat-management/magecart-growing-threat/ (last accessed July 8, 2020).

[11] While skimming attacks have become more popular, the practice of hackers using legitimate online services to host their infrastructure has expanded. Researchers at Malwarebytes recently discovered a rash of skimmers on the Heroku engagement platform, which is a PaaS run by Salesforce. This platform offers a free starter service for legitimate app developers to deploy, manage and scale their apps without needing to maintain their own infrastructure. Hackers are registering free accounts on Heroku to host their skimming schemes. Malwarebytes reported its findings to the Salesforce Abuse Operations team in late 2019. *There's an app for that: web skimmers found on PaaS Heroku*, Malwarebytes Labs, Dec. 4, 2019, *available at*: https://blog.malwarebytes.com/web-threats/2019/12/theres-an-app-for-that-web-skimmers-found-on-paas-heroku/ (last accessed July 10, 2020).

[12] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed July 8, 2020).

[13] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed July 8, 2020).

can also purchase access to entire company data breaches from $900 to $4,500.[14]

31. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding PII and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Defendant's customers as a result of a breach.

32. Defendant was, or should have been, fully aware of the significant volume of daily payment card transactions on Defendant's website—amounting to thousands of payment card transactions, and thus, the significant number of individuals who would be harmed by a breach of Defendant's systems.

Plaintiff Riggs' Experience

33. Plaintiff William Riggs purchased a product from iCanvas on May 27, 2020, for a total of $94.49. He checked out as a guest and used his Discover credit card.

34. On the payment platform, Mr. Riggs entered his PII: name, billing address, delivery address, payment card type and full number, CVV security code, payment card expiration date, and email address. During this transaction, Mr. Riggs was not asked to "agree" to any "Terms of Service" or to review the "Privacy Policy."

35. A few days after he made the purchase from iCanvas, Discover notified Mr. Riggs that there were suspicious charges on his credit card. Discover confirmed on June 23, 2020, that his card had been used by unauthorized third-parties multiple times.

36. Discover changed Mr. Riggs' account number in response to the illegal charges and mailed him a new card. Mr. Riggs had to take time out of his day to deal with the fraudulent charges and the account number change; time he otherwise would have spent performing other activities, such as his job and/or leisurely activities for the enjoyment of life. He also had to use alternative methods of payment until he received his new credit card.

37. On or about June 26, 2020, iCanvas notified Mr. Riggs by U.S. mail of the Data Breach in the *Notice of Data Breach*. He did not receive notice by email.

[14] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed July 8, 2020).

38. In response to the *Notice of Data Breach*, Mr. Riggs again had to spend time dealing with the consequences of the Data Breach, which includes time reviewing the account compromised by the Data Breach (which was his Discover credit card), contacting his bank, exploring credit monitoring options, and self-monitoring his accounts. This is time Mr. Riggs otherwise would have spent performing other activities, such as his job and/or leisurely activities for the enjoyment of life.

39. Knowing that the hacker stole his PII, and that his PII may be available for sale on the dark web, has caused Mr. Riggs great concern. He is now very concerned about credit card theft and identity theft in general. This breach has given Mr. Riggs hesitation about using iCanvas' services, and reservations about shopping on other online websites.

40. Now, due to Defendant's misconduct and the resulting Data Breach, hackers obtained his PII at no compensation to Mr. Riggs whatsoever. That is money lost for him, and money gained for the hackers, who could sell his PII on the dark web.

41. Mr. Riggs also suffered actual injury and damages in paying money to, and purchasing products from, Defendant's website during the Data Breach, expenditures which he would not have made had Defendant disclosed that it lacked computer systems and data security practices adequate to safeguard customers' PII from theft.

42. Moreover, Mr. Riggs suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of criminals.

43. Plaintiff Riggs has a continuing interest in ensuring his PII, which remains in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Riggs' Efforts to Secure PII

44. Defendant's Data Breach caused Mr. Riggs harm.

45. Prior to the activity described above during the period in which the Data Breach occurred, the Discover credit card that Mr. Riggs used to purchase products on Defendant's website had never been stolen or compromised. Mr. Riggs reviewed his credit reports and other financial statements routinely and to his knowledge this card had not been compromised in any

manner.

46. Additionally, Mr. Riggs never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

47. Mr. Riggs stores any and all electronic documents containing his PII in a safe and secure location, and destroys any documents he receives in the mail that contain any of his PII, or that may contain any information that could otherwise be used to compromise his credit card.

V. CLASS ALLEGATIONS

48. Plaintiff brings this nationwide class action on behalf of himself and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

49. The Nationwide Class that Plaintiff seeks to represent is defined as follows: **All individuals whose PII was compromised in the data breach first announced by iCanvas on June 24, 2020 (the "Nationwide Class").**

50. The Florida Subclass is initially defined as follows: **All persons residing in Florida whose PII was compromised in the data breach first announced by iCanvas on June 24, 2020 (the "Florida Subclass").**

51. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, current or former employees, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to its departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as Defendant's immediate family members.

52. Plaintiff reserves the right to modify or amend the definition of the proposed Classes before the Court determines whether certification is appropriate.

53. Numerosity, Fed R. Civ. P. 23(a)(1): The Nationwide Class and Florida Subclass (the "Classes") are so numerous that joinder of all members is impracticable. Defendant has identified thousands of customers whose PII may have been improperly accessed in the Data

Breach, and the Classes are apparently identifiable within Defendant's records.

54. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and when Defendant actually learned of the Data Breach and whether its response was adequate;

b. Whether Defendant owed a duty to the Classes to exercise due care in collecting, storing, safeguarding and/or obtaining their PII;

c. Whether Defendant breached that duty;

d. Whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of storing Plaintiff's and Class Members' PII;

e. Whether Defendant acted negligently in connection with the monitoring and/or protecting of Plaintiff's and Class Members' PII;

f. Whether Defendant knew or should have known that they did not employ reasonable measures to keep Plaintiff's and Class Members' PII secure and prevent loss or misuse of that PII;

g. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

h. Whether Defendant caused Plaintiff and Class Members damages;

i. Whether Plaintiff and the other Class Members are entitled to credit monitoring and other monetary relief;

j. Whether Defendant violated Florida's Deceptive and Unfair Trade Practices Act (Florida Statute § 501.203, *et seq.*).

55. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class Members because all had their PII compromised as a result of the Data Breach, due to Defendant's misfeasance.

56. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the

Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members, and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

57. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that he has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seek no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages he has suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex consumer class action litigation, and Plaintiff intends to prosecute this action vigorously.

58. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of class members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain class members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those class members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

59. The nature of this action and the nature of laws available to Plaintiff and the Class make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and the Class for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a

common course of conduct to which Plaintiff were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

60. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

61. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

62. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

63. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

64. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and the Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

b. Whether Defendant breached a legal duty to Plaintiff and the Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach; and

e. Whether Class Members are entitled to actual damages, credit monitoring or other injunctive relief, and/or punitive damages as a result of Defendant's wrongful conduct.

COUNT I

Negligence

(On Behalf of Plaintiff and the Nationwide Class)

65. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 64.

66. As a condition of their using Defendant's services, Plaintiff and Class Members were obligated to provide Defendant with the PII.

67. Plaintiff and the Class Members entrusted their PII to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

68. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed.

69. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of their customers' PII involved an unreasonable risk of harm to Plaintiff and Class Members, even if the harm occurred through the criminal acts of a third party.

70. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that Plaintiff and Class Members' information in Defendant's possession was adequately secured and protected.

71. Defendant also had a duty to have procedures in place to detect and prevent the

improper access and misuse of Plaintiff's and Class Members' PII.

72. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class Members was reasonably foreseeable, particularly in light of Defendant's inadequate information security practices.

73. Plaintiff and the Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew of should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendant's systems.

74. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and Class Members. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decisions not to comply with industry standards for the safekeeping of Plaintiff's and Class Members' PII.

75. Plaintiff and the Class Members had no ability to protect their PII that was in Defendant's possession.

76. Defendant was in a position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

77. Defendant had and continues to have a duty to adequately disclose that the PII of Plaintiff and Class Members within Defendant's possession might have been compromised, how it was compromised, and precisely the types of information that were compromised and when. Such notice was necessary to allow Plaintiff and the Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

78. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiff and Class Members.

79. Defendant has admitted that the PII of Plaintiff and Class Members was wrongfully disclosed to unauthorized third persons as a result of the Data Breach.

80. Defendant, through its actions and/or omissions, unlawfully breached its duties to

Plaintiff and Class Members by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiff and Class Members during the time the PII was within Defendant's possession or control.

81. Defendant improperly and inadequately safeguarded the PII of Plaintiff and Class Members in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

82. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect customers' PII in the face of increased risk of theft.

83. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of its customers PII.

84. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and Class Members the existence and scope of the Data Breach.

85. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and Class Members, the PII of Plaintiff and Class Members would not have been compromised.

86. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiff and Class Members and the harm suffered or risk of imminent harm suffered by Plaintiff and the Class. Plaintiff's and Class Members' PII was stolen and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

87. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent

researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of customers in its continued possession; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (ix) the diminished value of Defendant's goods and services they received.

88. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT II

Invasion of Privacy

(On Behalf of Plaintiff and the Nationwide Class)

89. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 64.

90. Plaintiff and Class Members had a legitimate expectation of privacy to their PII and were entitled to the protection of this information against disclosure to unauthorized third parties.

91. Defendant owed a duty to its customers, including Plaintiff and Class Members, to keep their PII contained as a part thereof, confidential.

92. Defendant failed to protect and released to unknown and unauthorized third parties the PII of Plaintiff and Class Members.

93. Defendant allowed unauthorized and unknown third parties unfettered access to and examination of the PII of Plaintiff and Class Members, by way of Defendant's failure to protect the PII.

94. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII of Plaintiff and Class Members is highly offensive to a reasonable person.

95. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and Class Members disclosed their PII to Defendant as part of their use of Defendant's services, but privately with an intention that the PII would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

96. Defendant's Data Breach constitutes an intentional interference with Plaintiff and Class Members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

97. Defendant acted with a knowing state of mind when they permitted the Data Breach to occur because they were with actual knowledge that its information security practices were inadequate and insufficient.

98. Because Defendant acted with this knowing state of mind, they had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiff and Class Members.

99. As a proximate result of the above acts and omissions of Defendant, the PII of Plaintiff and Class Members was disclosed to and used by third parties without authorization, causing Plaintiff and Class Members to suffer damages.

100. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class Members in that the PII maintained by Defendant can be viewed, distributed, and used by unauthorized persons. Plaintiff and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and the Class.

//

//

COUNT III

Negligence Per Se

(On Behalf of Plaintiff and the Nationwide Class)

101. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 64.

102. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

103. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, and the foreseeable consequences of the Data Breach for companies of Defendant's magnitude, including, specifically, the immense damages that would result to Plaintiff and Class Members.

104. Defendant's violations of Section 5 of the FTC Act constitute negligence *per se*.

105. Plaintiff and Class Members are within the class of persons that the FTC Act was intended to protect.

106. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class Members.

107. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts

spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of customers/patients and former customers/patients in its continued possession; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (ix) the diminished value of Defendant's goods and services they received.

108. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses

COUNT IV

Unjust Enrichment

(On Behalf of Plaintiff and the Nationwide Class)

109. Plaintiff re-alleges and incorporate by reference herein all of the allegations contained in paragraphs 1 through 64.

110. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they purchased goods and services from Defendant and provided Defendant with their PII. In exchange, Plaintiff and Class Members should have received from Defendant the goods and services that were the subject of the transaction and should have been entitled to have Defendant protect their PII with adequate data security.

111. Defendant knew that Plaintiff and Class Members conferred a benefit on Defendant and accepted and have accepted or retained that benefit. Defendant profited from the purchases and used the PII of Plaintiff and Class Members for business purposes.

112. The amounts Plaintiff and Class Members paid for Defendant's goods and services should have been used, in part, to pay for the administrative costs of data management and security.

113. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendant failed to implement the data management and security measures that are mandated by industry standards.

114. Defendant failed to secure the PII of Plaintiff and Class Members and, therefore, did not provide full compensation for the benefit Plaintiff and Class Members provided.

115. Defendant acquired the PII through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

116. If Plaintiff and Class Members knew that Defendant would not secure their PII using adequate security, they would not have made purchases with Defendant.

117. Plaintiff and Class Members have no adequate remedy at law.

118. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of customers/patients and former customers/patients in its continued possession; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (ix) the diminished value of Defendant's goods and services they received.

119. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including,

but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

120. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant's goods and services.

COUNT V

Declaratory Judgment

(On Behalf of Plaintiff and the Nationwide Class)

121. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 64.

122. Defendant owes duties of care to Plaintiff and Class Members which would require it to adequately secure PII.

123. Defendant still possesses PII regarding Plaintiff and Class Members.

124. Plaintiff and Class Members' PII is still for sale on the dark web.

125. Although Defendant claims it "took certain technical precautions to prevent this type of incident from occurring again," there is no detail on what, if any, fixes have really occurred.

126. Plaintiff and Class Members are at risk of harm due to the exposure of their PII and Defendant's failure to address the security failings that lead to such exposure.

127. There is no reason to believe that Defendant's security measures are any more adequate than they were before the Data Breach to meet Defendant's contractual obligations and legal duties, and there is no reason to think Defendant has no other security vulnerabilities that have not yet been knowingly exploited.

128. Plaintiff, therefore, seek a declaration that: (1) each Defendant's existing security measures do not comply with Defendant's explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices appropriate to the nature of the information to protect customers' personal information; and (2) to comply with Defendant's

explicit or implicit contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

a. Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendant audit, test, and train Defendant's security personnel regarding any new or modified procedures;

d. Ordering that Defendant user applications be segmented by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendant's systems;

e. Ordering that Defendant conduct regular database scanning and securing checks;

f. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

g. Ordering Defendant to purchase credit monitoring services for Plaintiff and Class Members for a period of ten years; and

h. Ordering Defendant to meaningfully educate Defendant's users about the threats they face as a result of the loss of their PII to third-parties, as well as the steps Defendant's customers must take to protect themselves.

//

//

COUNT VI

Violation of Florida's Deceptive and Unfair Trade Practices Act,

Florida Statute § 501.203, *et seq*.

(On Behalf of Plaintiff and the Nationwide Class, or in the alternative,

On Behalf of Plaintiff and the Florida Subclass)

129. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 64.

130. Plaintiff and the Class Members are "consumers." Fla. Stat. § 501.203(7).

131. Plaintiff and Class Members purchased "things of value" insofar as products and services from Defendant. These purchases were made primarily for personal, family, or household purposes. Fla. Stat. § 501.203(9).

132. Defendant engaged in the conduct alleged in this Complaint by advertising and entering into transactions intended to result, and which did result, in the sale, rental of goods, services, and/or property to consumers, including Plaintiff and the Class Members. Fla. Stat. § 501.203(8).

133. Defendant engaged in, and its acts and omissions affected trade and commerce. Defendant's acts, practices, and omissions were done in the course of Defendant's business of advertising, marketing, offering to sell, and selling and/or renting goods and services throughout Florida and the United States. Fla. Stat. § 501.203(8).

134. Defendant, operating in Florida and elsewhere through its worldwide website, engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce, in violation of Fla. Stat. § 501.204(1), including but not limited to the following:

a. charging a premium for the goods and services, implicitly representing that the premium would be used to protect Plaintiff's and Class Members' protected health information and other PII;

b. continued acceptance of credit and debit card payments and storage of other PII after Defendant knew or should have known of the Data Breach and before they allegedly remediated the Data Breach.

135. This conduct is considered unfair methods of competition, and constitutes unfair and unconscionable acts and practices. Fla. Stat. § 501.204(1).

136. As a direct and proximate result of Defendant's violation of Florida's Deceptive and Unfair Trade Practices Act ("FDUTPA"), Plaintiff and the Class Members suffered actual damages by paying a premium for Defendant's goods and services with the understanding that at least part of the premium would be applied toward sufficient and adequate information security practices that comply with industry standards, when in fact no portion of that premium was applied toward sufficient and adequate information security practices. Fla. Stat. § 501.211(2).

137. Moreover, as a direct result of Defendant's knowing violation of FDUTPA, Plaintiff and Class Members are not only entitled to actual damages, but also declaratory judgment that Defendant's actions and practices alleged herein violate FDUTPA, and injunctive relief, including, but not limited to:

a. Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures;

d. Ordering that Defendant segment PII by, among other things, creating firewalls and access controls so that if one area of Defendant is compromised, hackers cannot gain access to other portions of Defendant's systems;

e. Ordering that Defendant purge, delete, and destroy in a reasonable secure manner PII not necessary for its provisions of services;

f. Ordering that Defendant conduct regular database scanning and securing checks;

g. Ordering that Defendant routinely and continually conduct internal training and

education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. Ordering Defendant to meaningfully educate its customers about the threats they face as a result of the loss of their financial and personal information to third-parties, as well as the steps Defendant's customers must take to protect themselves.

Fla. Stat. § 501.211(1).

138. Plaintiff brings this action on behalf of themselves and the Class Members for the relief requested above and for the public benefit to promote the public interests in the provision of truthful, fair information to allow consumers to make informed purchasing decisions and to protect Plaintiff and the Class Members and the public from Defendant's unfair methods of competition and unfair, deceptive, fraudulent, unconscionable, and unlawful practices. Defendant's wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

139. The above unfair and deceptive practices and acts by Defendant were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and the Class Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

140. Defendant knew or should have known that the lack of encryption on its computer systems and data security practices were inadequate to safeguard the Class Members' PII and that the risk of a data disclosure or theft was high.

141. Defendant's actions and inactions in engaging in the unfair practices and deceptive acts described herein were negligent, knowing and willful, and/or wanton and reckless.

Plaintiff and the Class Members seek relief under Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. §§ 501.201, *et seq.*, including, but not limited to, damages, injunctive relief, and attorneys' fees and costs, and any other just and proper relief.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all Class Members, requests judgment against the Defendant and that the Court grant the following:

A. An order certifying the Nationwide Class and Florida Subclass as defined herein,

and appointing Plaintiff and his Counsel to represent the Class;

B. An order enjoining Defendant from engaging in the wrongful conduct alleged herein concerning disclosure and inadequate protection of Plaintiff's and Class Members' PII;

C. An order instructing Defendant to purchase or provide funds for credit monitoring services for Plaintiff and all Class Members;

D. An award of compensatory, statutory, and punitive damages, in an amount to be determined;

E. An award for equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

F. An award of reasonable attorneys' fees, costs, and litigation expenses, as allowable by law; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Date: July 14, 2020

Respectfully Submitted,

By: */s/ Leslie Guillon*_____
Leslie Guillon (SBN 222400)
lguillon@justice4you.com
M. Anderson Berry (SBN 262879)
aberry@justice4you.com
CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 777-7777
Facsimile: (916) 924-1829